DRAFT NISTIR 8114

Report on Lightweight Cryptography

Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha

National Institute of
Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8114

Report on Lightweight Cryptography

Kerry A. McKay
Larry Bassham
Meltem Sönmez Turan
Nicky Mouha
Computer Security Division
Information Technology Laboratory

August 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8114
29 pages (August 2016)

Public comment period: August 11, 2016 through October 31, 2016

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: lightweight-crypto@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

NIST-approved cryptographic standards were designed to perform well using general-purpose computers. In recent years, there has been increased deployment of small computing devices that have limited resources with which to implement cryptography. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project that was tasked with learning more about the issues and developing a strategy for the standardization of lightweight cryptographic algorithms. This report provides an overview of the lightweight cryptography project at NIST, and describes plans for the standardization of lightweight cryptographic algorithms.

Keywords

Constrained devices; lightweight cryptography; standardization

Acknowledgements

The authors would like to thank their NIST colleagues for providing valuable feedback during the development of this publication.

Executive Summary

There are several emerging areas in which highly constrained devices are interconnected, working in concert to accomplish some task. Examples of these areas include: automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the constrained devices used by these applications. When current NIST-approved algorithms can be engineered to fit into the limited resources of constrained environments, their performance may not be acceptable. For these reasons, NIST started a lightweight cryptography project that was tasked with learning more about the issues and developing a strategy for the standardization of lightweight cryptographic algorithms.

This report provides an overview of lightweight cryptography, summarizes the findings of the NIST's lightweight cryptography project, and outlines NIST's plans for the standardization of lightweight primitives. In particular, NIST has decided to create a portfolio of lightweight primitives through an open process similar to the selection of block cipher modes of operation. Algorithms will be recommended for use only in the context of profiles, which describe physical, performance, and security characteristics. These profiles are intended to capture cryptographic algorithm requirements imposed by devices and applications where lightweight cryptography is needed. NIST will develop profiles based on community responses to questions, included in this report, about application and device requirements for lightweight cryptography.

Table of Contents

1 Introduction

The deployment of small computing devices such as RFID tags, industrial controllers, sensor nodes and smart cards is becoming much more common. The shift from desktop computers to small devices brings a wide range of new security and privacy concerns. It is challenging to apply conventional standards to small devices. In many conventional cryptographic standards, the tradeoff between security, performance and resource requirements was optimized for desktop and server environments, and this makes them difficult or impossible to implement in resource-constrained devices. When they can be implemented, their performance may not be acceptable.

Lightweight cryptography is a subfield of cryptography that aims to provide solutions tailored for resource-constrained devices. There has been a significant amount of work done by the academic community related to lightweight cryptography; this includes efficient implementations of conventional cryptography standards, and the design and analysis of new lightweight primitives and protocols.

In 2013, NIST initiated a lightweight cryptography project to study the performance of the current NIST-approved cryptographic standards on constrained devices and to understand the need for dedicated lightweight cryptography standards, and if the need is identified, to design a transparent process for standardization. In 2015, NIST held the first Lightweight Cryptography Workshop in Gaithersburg, MD, to get public feedback on the constraints and limitations of the target devices, and requirements and characteristics of real-world applications of lightweight cryptography.[1]

Recently, NIST has decided to create a portfolio of lightweight primitives through an open process similar to the selection of modes of operation of block ciphers [48]. In this report, we aim to summarize the finding of the lightweight cryptography project and outline NIST's plans for the standardization of lightweight primitives. This report also includes a list of questions to the stakeholders of lightweight cryptography that will serve as the basis for determining requirements. Responses to the questions should be sent to lightweight-crypto@nist.gov with the subject line "Responses to questions on lightweight crypto requirements" before October 1, 2016.

The remainder of this report is organized as follows. Section 2 provides an overview of lightweight cryptography, including metrics and developments. Section 3 provides information about NIST's lightweight cryptography project, including the proposed path for the standardization of lightweight algorithms, design considerations, and a profile template that will be used in the evaluation process.

[1] For workshop presentations, visit http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm.

2 Overview of Lightweight Cryptography

This section introduces various aspects of lightweight cryptography, including target devices, performance metrics, applications and dedicated designs.

2.1 Target Devices

Lightweight cryptography targets a wide variety of devices that can be implemented on a broad spectrum of hardware and software. On the high end of the device spectrum are servers and desktop computers followed by tablets and smartphones. Conventional cryptographic algorithms may perform well in these devices; therefore, these platforms may not require lightweight algorithms. Finally, on the lower end of the spectrum are devices such as embedded systems, RFID devices and sensor networks. Lightweight cryptography is primarily focused on the highly constrained devices that can be found in the lower end of this spectrum.

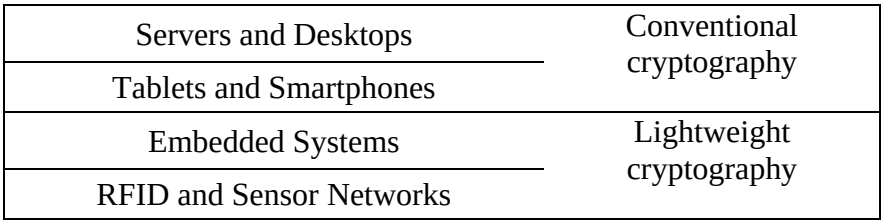

Figure 1 Device Spectrum

Microcontrollers are available with a wide array of performance attributes. Although 8-bit, 16-bit and 32-bit microcontrollers are the most common, there are significant sales of 4-bit microcontrollers for certain ultra-low cost applications. A wide variety of instruction sets exist, typically only simple instructions are supported, and the number of instructions is often very limited. This may result in a high number of cycles to execute common cryptographic algorithms, which may make them too slow or energy-consuming for the intended application. This is particularly a problem when it is necessary to satisfy real-time constraints using a limited amount of energy.

For some microcontrollers, the amount of RAM and ROM can be extremely limited. For example, the TI COP912C [62] has 64 bytes of RAM, and the NXP RS08 [52] can have as little as 63 bytes of RAM. The Microchip PIC10/12/16 microcontrollers [45] exist in many variants with 64 bytes of RAM and less, going down to as little as 16 bytes of RAM.

On the bottom of the spectrum there are RFID and sensor networks, which are often realized in hardware (ASIC) in order to satisfy some of the most stringent implementation constraints. Of particular interest are UHF RFID tags, for example using the widely deployed EPCGlobal Gen2 [22] and ISO/IEC 18000-63 [39] standards.

For RFID tags that are not battery-powered, only a limited amount of power is available from the environment. Such devices require cryptographic algorithms that are not only implemented with a very small amount of gate equivalents (GEs), but must meet stringent timing and power

requirements as well. A study of the constraints of such devices for cryptographic applications was performed in [57].

Lightweight algorithms may be subject to various other constraints, a topic that will be explored during the first phase of the standardization effort. The aforementioned examples are therefore not intended to be exhaustive list, but to illustrate settings where conventional algorithms cannot be implemented, in order to understand the need for lightweight alternatives.

2.2 Performance Metrics

In cryptographic algorithm design, there is a tradeoff between the performance and the resources required for a given security level. Performance can be expressed in terms such as power and energy consumption, latency, and throughput. The resources required for a hardware implementation are usually summarized in gate area, gate equivalents, or slices. In software this is reflected in register, RAM and ROM usage. Resource requirements are sometimes referred to as costs, as adding more gates or memory tends to increase the production cost of a device.

Power and energy consumption are relevant metrics due to the nature of many constrained devices. Power may be of particular importance in devices that harvest power from their surroundings. An example would be an RFID chip that uses the electromagnetic field transmitted by a reader to power its internal circuit. Energy consumption (i.e., power consumption over a certain time period) is especially important in battery-operated devices that have a fixed amount of stored energy. The batteries in some devices may be difficult or impossible to recharge or replace once deployed. It should also be noted that power consumption depends on many factors, such as the threshold voltage, the clock frequency and the technology used for implementation.

Latency is especially relevant for certain real-time applications, for example automotive applications where very fast response times for components such as steering, airbags or brakes are required. It can be defined as the measure of time between initial request of an operation and producing the output. For example, the latency of an encryption operation is the time between the initial request for encryption of a plaintext and the reply that returns the corresponding ciphertext.

Throughput is the rate at which new outputs (e.g., authentication tags or ciphertext) are produced. Unlike conventional primitives, high throughput may not be a design goal in lightweight designs. However, moderate throughput is still required in most applications.

2.2.1 Hardware-Specific Metrics

Resource requirements for hardware platforms are typically described in terms of gate area. The area of an implementation depends on the technology and the standard cell library, and is measured in μm^2. Area can be stated in terms of slices for FPGAs, or by *gate equivalents* (GEs) for ASIC implementation.

On FPGAs, a slice is the basic reconfigurable unit, that contains a number of look-up tables (LUTs), flip-flops and multiplexers. Slices are implemented differently on different FPGAs. The

number of LUTs, flip-flops and multiplexers depends on the FPGA family, as well as the number of input and output bits of the LUTs.

For ASICs, one GE is equivalent to the area that is required by the two-input NAND gate. The area in GE is obtained by dividing the area in μm^2 by the area of the NAND gate. The number of GEs of a hardware implementation is therefore very specific to a particular technology, so that it is not possible to directly compare the number of GEs of implementations across different technologies.

A low-cost RFID tag may have a total gate count of 1,000-10,000 gates, out of which only 200-2,000 may be used for security purposes [41]. Area requirements and power consumption can be correlated, in which case minimizing area also tends to reduce the power consumption.

2.2.2 Software-Specific Metrics

For software applications, resource requirements can be measured by the number of registers, as well as the number of bytes of RAM and ROM that are required. Functions that use a small number of registers have a lower calling overhead, as fewer variables must be placed on the stack before the registers can be overwritten. ROM is used to store the program code, and can include fixed data, such as S-boxes or hardcoded round keys, while RAM is used to store intermediate values that can be used in computations. This can lead to additional tradeoffs between calculating values on the fly versus looking up values in a table.

2.3 Lightweight Cryptographic Primitives

Over the last decade, a number of lightweight crypto primitives (including block ciphers, hash functions, message authentication codes and stream ciphers) have been proposed to bring performance advantages over conventional cryptographic standards. These primitives differ from conventional algorithms with the assumptions that lightweight primitives are not intended for a wide range of applications, and may impose limits on the power of the attacker. For example, the amount of data available to the attacker under a single key may be limited. However, it should be noted that this does not mean that the lightweight algorithms are weak – rather the idea is to use advancements to result in designs with a better balance between security, performance, and resource requirements for specific resource-constrained environments.

2.3.1 Lightweight Block Ciphers

A number of lightweight block ciphers have been proposed to achieve performance advantages over NIST's Advanced Encryption Standard (AES)[63], particularly AES-128. Some of these ciphers were designed by simplifying conventional, well-analyzed block ciphers to improve their efficiency. As an example, DESL [42] is a variant of DES, where the round function uses a single S-box instead of eight and omits the initial and final permutations to improve the size of the hardware implementation. Alternatively, some of the algorithms are dedicated block ciphers that were designed from scratch. PRESENT [8] is one of the first lightweight block cipher designs that was proposed for constrained hardware environments. SIMON and SPECK [6] are families of lightweight block ciphers that were designed to be simple, flexible, and perform well

in hardware and software. There are also algorithms from 1990s such as RC5 [56], TEA [68] and XTEA [51], which consist of simple round structures that make them suitable for constrained software environments. A non-exhaustive list of lightweight block ciphers is provided in [67].

The performance benefits of lightweight block ciphers over conventional block ciphers are achieved using lightweight design choices, such as:

- ***Smaller block sizes:*** To save memory, lightweight block ciphers may use smaller block sizes than AES (e.g., 64 or 80 bits, rather than 128). It should also be noted that using small block sizes reduces limits on the length of the plaintexts to be encrypted. For example, outputs of a 64-bit block cipher can be distinguished from a random sequence using around 2^{32} blocks for some of the approved modes of operations. Depending on the algorithm, this may lead to plaintext recovery, key recovery or authentication tag forgeries with non-negligible probabilities.

- ***Smaller key sizes:*** Some lightweight block ciphers use small key sizes (less than 96 bits) for efficiency (e.g., 80-bit PRESENT). At the time of this writing, the minimum key size required by NIST is 112 bits [4].

- ***Simpler rounds:*** The components and operations used in lightweight block ciphers are typically simpler than those of conventional block ciphers. In lightweight designs using S-boxes, 4-bit S-boxes are preferred over 8-bit S-boxes. This reduction in size results in significant area savings. For example, the 4-bit S-box used in PRESENT required 28GEs, whereas AES S-box required 395 GEs in [20]. For hardware-oriented designs, bit permutations (such as those used in PRESENT), or recursive MDS matrices (as in PHOTON [23] and LED [24]) may be preferred over complex linear layers. When rounds are simpler, they may need to be iterated more times to achieve security.

- ***Simpler key schedules:*** Complex key schedules increase the memory, latency and the power consumption of implementations; therefore, most of the lightweight block ciphers use simple key schedules that can generate sub-keys on the fly. This may enable attacks using related keys, weak keys, known keys or even chosen keys. When this is the case, it is necessary to ensure that all keys are generated independently using a secure key derivation function (KDF) [10, 11, 14, 60].

2.3.2 Lightweight Hash Functions

Conventional hash functions may not be suitable for constrained environments, mainly due to their large internal state sizes and high power consumption requirements. This has led to the development of lightweight hash functions, such as PHOTON [23], Quark [2] SPONGENT [7], and Lesamnta-LW [26]. The expected usage of conventional and lightweight hash functions differs in various aspects such as [54]:

- ***Smaller internal state and output sizes:*** Large output sizes are important for applications that require collision resistance of hash functions. For applications that do not require collision resistance, smaller internal and output sizes might be used. When a collision-

resistant hash function is required, it may be acceptable that this hash function has the same security against preimage, second-preimage and collision attacks. This may reduce the size of the internal state.

- ***Smaller message size:*** Conventional hash functions are expected to support inputs with very large sizes (around 2^{64} bits). In most of the target protocols for lightweight hash functions, typical input sizes are much smaller (e.g., at most 256 bits). Hash functions that are optimized for short messages may therefore be more suitable for lightweight applications.

2.3.3 Lightweight Message Authentication Codes

A message authentication code (MAC) generates a tag from a message and a secret key, which is used to verify the authenticity of the message. Tag sizes are recommended to be at least 64 bits for typical applications. For certain applications such as VoIP (Voice over IP), occasionally accepting an inauthentic message may have limited impact on the security of the application, so that shorter tags can be used after careful consideration. Chaskey [47], TuLP [21], and LightMAC [43] are some of the examples of lightweight MAC algorithms.

2.3.4 Lightweight Stream ciphers

Stream ciphers are also promising primitives for constrained environments. The eSTREAM competition [19], organized by the European Network of Excellence for Cryptology, aimed to identify new stream ciphers that might be suitable for widespread adoption. The finalists of the competition were announced in 2008 and included three stream ciphers for hardware applications with restricted resources:

- *Grain* [25] is widely analyzed and provides implementation flexibility, and also has a version that supports authentication.

- *Trivium* [15] is a widely analyzed, elegant and flexible design; however, it only supports 80-bit keys.

- *Mickey* [3] is less analyzed compared to Grain and Trivium, and its security mostly depends on the hardness of analysis. It provides less implementation flexibility and susceptible to timing and power analysis, due to irregular clocking.

2.4 NIST-Approved Cryptographic Primitives in Constrained Environments

This section discusses the performance of NIST-approved cryptographic standards in resource-constrained environments.

- ***Block ciphers:*** There are two NIST-approved block cipher algorithms; AES and Triple DES (TDEA)[5].[2] The AES family of block ciphers includes three variants AES-128, AES-192, and AES-256 that support key sizes of 128, 192 and 256 bits, respectively. All AES variants operate have a block size of 128 bits. For lightweight cryptography purposes, the most suitable variant of the family is AES-128, due to the number of rounds and size of the key schedule. Existing compact implementations of AES-128 require 2090 GEs [44] to 2400 GEs [46]. AES is mainly designed for software applications. Using 8-bit AVR microcontrollers, encryption has been achieved in cycles per byte 124.6 and decryption in 181.3 cycles per byte, with a code size less than 2 Kbyte [53]. AES performs very well on certain 8-bit microcontrollers, making it a good choice for those platforms. Both encryption and decryption operations in block ciphers such as AES and Triple-DES cannot be implemented on a Renesas RL78 16-bit microcontroller [55] when the amount of ROM is limited to 512 bytes and RAM is limited to 128 bytes [13]. For applications where the performance of AES is acceptable, AES should be used for encryption.

- ***Hash functions:*** NIST-approved hash functions are specified in two FIPS standards: FIPS 180-4 [65] specifies SHA-1,[3] the SHA-2 family (namely, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512-224 and SHA-512/256) and FIPS 202 [66] specifies the permutation-based SHA-3 family (namely, SHA3-224, SHA3-256, SHA3-384, and SHA3-512). None of these approved hash functions are suitable for use in very constrained environments, mainly due their large internal-state size requirements. Ideguchi et al. [27] studied the RAM requirements of SHA-256, SHA-512 and various SHA-3 candidates on low-cost 8-bit microcontrollers, and found that none of the NIST-approved hash functions could be implemented within 64 bytes of RAM. The internal state size for the SHA-3 family is mainly determined by the width of the underlying 1600-bit permutation. FIPS 202 additionally defines smaller-sized permutations with sizes 25, 50, 100, 200, 400, and 800; some of these variants may later be used to define lightweight variants of SHA-3, however currently these smaller variants are not approved for use in hash functions.

- ***Authenticated Encryption and MACs:*** Authenticated encryption provides performance and resource requirement advantages, because it simultaneously provides confidentiality and integrity protection of messages. NIST approves the CCM [16] and GCM [18] block cipher modes that provide authentication and encryption simultaneously. NIST also approves standalone MACs, CMAC [17], GMAC [18], and HMAC [64], to be used for generating and verifying message authentication.

2.5 Lightweight Cryptography Standards

ISO/IEC 29192, *Lightweight Cryptography*, is a six-part standard that specifies lightweight

[2] A third block cipher, Skipjack, is only approved for legacy-use decryption. See [SP800-131A] for more information.

[3] SHA-1 is not approved for all common uses of a hash function. See [4] for further details.

cryptographic algorithms for confidentiality, authentication, identification, non-repudiation, and key exchange. Part 1 [28] includes general information such as security, classification and implementation requirements. Part 2 specifies the block ciphers PRESENT and CLEFIA [29]. Part 3 specifies the stream ciphers Enocoro and Trivium [ISO29192-3]. Part 4 specifies three asymmetric techniques namely (*i*) identification scheme cryptoGPS, (*ii*) authentication and key exchange mechanism ALIKE, and (*iii*) ID-based signature scheme IBS [30]. Part 5 specifies three hash functions: PHOTON, SPONGENT, and Lesamnta-LW [40]. Part 6 is dedicated to MACs and is currently under development.

ISO/IEC 29167, *Automatic Identification and Data Capture Techniques*, provides security services for RFID air interface communications. Part 1 [31] describes the architecture, security features, and requirements for security services for RFID devices. Crypto suites are defined in additional parts. Currently, seven suites are published in [32-38]. Additional documents are under development.

Cryptography Research and Evaluation Committees (CRYPTREC) is a project to evaluate and monitor security of cryptographic techniques used in Japanese e-Government systems [12]. CRYPTREC publishes three types of cipher lists: e-Government Recommended Ciphers List, Candidate Recommended Ciphers List and Monitored Ciphers List. The Lightweight Cryptography working group of CRYPTREC, established in 2013, aims to study and support appropriate lightweight cryptography solutions for e-government systems and any applications where lightweight solutions are needed. The working group surveys research on state of the art in lightweight cryptography and its applications, and performs implementation evaluations, and published a report (in Japanese) [13] as a deliverable in 2015. The target algorithms for implementation in the report were AES, Camellia [1], CLEFIA [59], PRESENT [8], LED [24], Piccolo [58], TWINE [61], and PRINCE [9].

3 NIST's Lightweight Cryptography Project

NIST develops standards using several different approaches, as described in [50]. NIST has held competitions to select the AES block cipher and the SHA-3 hash functions. These competitions were significant efforts that took place over many years. For example, the SHA-3 competition was announced in 2007, the winner was announced in 2012, and the standardization process was concluded in 2015. Another approach is to adapt standards of other accredited standards development organizations, as was done with HMAC and RSA standards. NIST researchers also develop standards and guidelines in collaboration with experts in academia, industry and government, if no suitable standard exists.

The landscape for lightweight cryptography is moving so quickly that a standard produced using the competition model is likely to be outdated prior to standardization. Therefore, the most suitable approach for lightweight cryptography, in terms of timeline and project goals, is to develop new recommendations using an open call for proposals to standardize algorithms.

NIST is planning to develop and maintain a portfolio of lightweight primitives and modes that are approved for limited use. Each algorithm in the portfolio will be tied to one or more *profiles*, which consist of algorithm goals and acceptable ranges for metrics. This is in contrast to other primitives and modes that are approved for general use. Any restrictions on use will be included in the recommendation or standard where the primitives and modes of the portfolio are specified. Algorithm transitions and deprecation guidance will be provided as algorithms in the portfolio are phased out. The lightweight portfolio is not intended to offer alternative algorithms for general use.

3.1 Scope and Design Considerations

The scope of NIST's lightweight cryptography project includes all cryptographic primitives and modes that are needed in constrained environments. However, the initial focus of the project is on block ciphers, hash functions, and message authentication codes. When long-term security is needed, these algorithms should either aim for post-quantum security [49], or the application should allow them to be easily replaceable by algorithms with post-quantum security.

While public key cryptography is not included in the initial focus, it is within the scope of this project. However, it should be noted that public key schemes will only be considered for inclusion in the portfolio under two conditions: 1) they are robust against quantum attacks, or 2) use a combination of general public key cryptographic schemes with lightweight primitives (e.g., lightweight hash function). Protocol design is also an important part of achieving the desired level of security while meeting requirements of a constrained environment, but is not within the scope of this project.

3.1.1 General Design Considerations

While specific requirements vary by application, there are several generally desired properties that NIST will be using to evaluate designs.

- ***Security strength*:** Any algorithm selected for the portfolio must provide adequate security. More specifically, the security strength should be at least 112 bits.

- ***Flexibility*:** Efficient implementations of an algorithm should be possible across an assortment of platforms. Algorithms should also allow a variety of implementations on a single platform. Tunable algorithms, which use parameters to select properties such as state size and key size, are desirable as they allow implementations with multiple options using fewer resources than multiple algorithms that do not share logic, thereby supporting a wider array of applications.

- ***Low overhead for multiple functions*:** Multiple functions (such as encryption and decryption) that share the same core are preferred over functions that have completely different logic. For example, a block cipher where the encryption and decryption operations use similar round functions may be preferable over one that has distinct round functions for encryption and decryption. Different primitives, such as a hash function and block cipher, can also share logic, thus reducing the resources needed to implement multiple algorithms in the same device.

- ***Ciphertext expansion*:** The size of the ciphertext has an impact on storage and transmission costs. Algorithms and modes that do not significantly increase the amount of data are desirable.

- ***Side channel and fault attacks*:** Implementations can leak sensitive information, particularly information about the key or plaintext, in a variety of ways. Side channel attacks use properties of the implementation during execution of the cryptographic operations, such timing, power consumption, and electromagnetic emissions, to discover this sensitive information. Fault attacks recover this sensitive information by introducing errors in the computation. In the case of pervasive devices, this is particularly notable as attackers may have physical access to the devices, and countermeasures for such attacks may not be present due to constrained resources. Algorithms that are easy to protect against side channel and fault attacks are desirable.

- ***Limits on the number of plaintext-ciphertext pairs*:** It may be permissible for algorithm designers to assume an upper bound on the number of plaintext/ciphertext pairs, as this limit can be justified for some applications by the constraints of the devices, (e.g., limitations on the amount of data that are processed by the same key), or message formats defined by protocols. However, it must be recognized that an attacker may mount attacks using plaintext that was encrypted under multiple, independent keys (multi-key attacks), which are relevant even when the amount of data encrypted under any single key is limited.

- ***Related-key attacks*:** These attacks allow an adversary to discover information about a key by performing operations using multiple keys that, although unknown, have a known relation. This is particularly a threat in protocols where keys are not chosen independent and at random. Keys may be permanently burned into the hardware of constrained devices, with no means of replacement. If this is the case, then related key attacks are only a practical threat if an adversary can obtain several devices that have keys with a known relation. This

446 attack model still remains highly relevant for devices where the capability to update the key
447 exists. The algorithms are expected to provide some resistance to related key attacks (e.g.,
448 attacks require large number of related keys).

449 It may not be possible to satisfy all properties, in particular when this increases the resources
450 beyond what is available for a given application. Still, any algorithm selected for the portfolio
451 must provide adequate security. In particular, the security against key-recovery attacks should be
452 at least 112 bits.

453 3.2 Profiles

454 NIST will evaluate and recommend algorithms based on profiles, which consist of a set of design
455 goals, physical characteristics of target devices, performance characteristics imposed by the
456 applications, and security characteristics.

457 Cryptographic primitives can be designed with a variety of goals in mind. The choices made in
458 the design goals can affect the various characteristics. Initially, this project will focus on block
459 ciphers, authenticated encryption schemes, hash functions, and message authentication codes.

460 Profiles should be designed to target classes of devices and applications – not necessarily
461 specific applications. Profiles should be useful across a variety of applications. The
462 characteristics that have been identified to be addressed in profiles are:

Physical characteristics	Performance characteristics	Security characteristics
Area (in GE)	Latency (in clock cycles)	Minimum security strength (bits)
Memory (RAM/ROM)	Throughput (cycles per byte)	Attack models
Implementation type (hardware, software, or both)	Power (μW)	Side channel resistance requirements

463

464 The appropriateness of an algorithm depends on the physical limitations of the device and the
465 performance and security objectives imposed by the application.

466 3.2.1 Profile Development

467 When building profiles for lightweight cryptography, the numbers that express the physical,
468 performance and security characteristics that apply to a specific constrained environment may
469 not be meaningful by themselves. The reasoning behind them needs to be understood as well.

470 Questions on Application and Device Requirements

471 To develop profiles, NIST asks a series of questions to the stakeholders of lightweight

cryptography, in order to build relevant profiles for a variety of applications. This may help to get a thorough understanding of a particular application and to identify the bottlenecks, or even to identify additional constraints that are not immediately apparent. Responses to the questions should be sent to lightweight-crypto@nist.gov with the subject line "Responses to questions on lightweight crypto requirements" before October 1, 2016.

The list of questions is as follows. For a given application environment, not all questions may apply.

1. What is the target application?
2. What types of functionality are required by the application (e.g., encryption, authentication, hashing, signatures, etc.)?
3. Are any cryptographic algorithms currently used by the application? If so, which algorithms? What motivated the choice for these algorithms? If not, why were certain algorithms found to be unsuitable?
4. Are the algorithms mainly used locally (e.g., the direct communication between a tag and a reader), or over a network?
5. Given the application, how difficult is it to replace a cryptographic algorithm?
6. Does the application mainly target hardware or software implementation, or are both equally relevant? If so, why?
7. If software implementations are relevant, what platforms are considered (server, desktop, laptop, smartphone, embedded, etc.)? Which specific types of processors (vendor and architecture) are the main targets?
8. If hardware implementations are relevant, which types of hardware are considered (FPGA, ASIC, etc.)? Which specific platforms are under consideration (vendor, architecture, technology, standard-cell library, etc.)?
9. For software implementations, which resources are available for the cryptographic computation? Are there limits on the amount of registers, RAM and ROM that are available? If so, what technological or practical considerations can explain these limits?
10. For hardware implementations, are there limits on the amount of slices or GEs that are available for the implementation? If so, what technological or practical considerations can explain these limits?
11. Is the platform an inherently serial one, or can data be processed in parallel?
12. Is built-in support for cryptographic operations available on the platform? (Hardware security modules, cryptographic instructions, cryptographically secure random or pseudo-random bit generators?)
13. In the case of software implementations, is it necessary to obfuscate the implementation? If so, why?
14. Is resistance against side-channel or fault attacks required? If no, why not?
15. Is some user-programmable non-volatile memory available?
16. How are keys generated? Where are they stored, and for how long?
17. How much data is processed under the same key? Are there inherent limitations to the amount of data that is processed, e.g. resulting from the protocol or from technical constraints?
18. Are the devices battery-powered, or do they draw their current from the environment? What limits are imposed on the energy and/or power that is available to the device?

19. Does the device have to respond within a specific time? Is this a soft real-time (reduced usefulness after the deadline) or hard real-time (data becomes useless after deadline) requirement? How do these requirements translate to restrictions on any cryptographic algorithms that may be used in the application?
20. What are typical sizes for a plaintext, ciphertext, message, authentication tag, etc.? What technological or practical factors determine their size? Would ciphertext expansion be acceptable, and if so by how many bytes?
21. What are the concrete requirements for the security of the application? Which types of attacks are considered to be relevant, or irrelevant for the given application? Why so?
22. Is there any other information that can be relevant to understand the application from a security or efficiency point of view?

3.2.2 Profile Template and Sample Profiles

It is not expected that one algorithm will necessarily meet all characteristics goals simultaneously. As such, profiles will be developed to support a set of characteristics and design goals. The proposed template is as follows:

Profile <*profile name*>	
Primitive	*Type of primitive*
Physical characteristics	*Name physical characteristic(s), and provide acceptable range(s) (e.g., 64 to 128 bytes of RAM)*
Performance characteristics	*Name performance characteristic(s), and provide acceptable range(s) (e.g., latency of no more than 5 ns)*
Security characteristics	*Minimum security strength, relevant attack models, side channel resistance requirements, etc.*
Design goals	*List design goals.*

The following sample profiles are provided for example purposes only. Profiles for inclusion in the portfolio will be developed with the community in an open process. Sample applications are provided, but selected algorithms should be suitable for a variety of applications.

Sample Profile #1

The first sample profile is for a MAC algorithm having a low-area implementation in hardware, and is designed for short input messages.

Profile Sample_1	
Primitive	MAC
Physical characteristics	1600 to 1900 GEs, ASIC hardware implementation
Performance characteristics	Latency ≤ 15 ns
Security characteristics	128-bit security, resistance to related key attacks, timing analysis
Design goals	Efficient for short input messages

A sample application using profile Sample_1 would be an RFID tag for asset tracking.

Sample Profile #2

The second sample profile is for an authenticated encryption algorithm with low latency. The implementation may be in hardware or software, but should allow for decryption/verification.

Profile Sample_2	
Primitive	Block cipher
Physical characteristics	Hardware or software implementation
Performance characteristics	Latency ≤ 20 ns
Security characteristics	128-bit security, resistance to power analysis
Design goals	Authenticated encryption

A sample application using profile Sample_2 would be command validation on a Controller Area Network (CAN) bus.

Sample Profile #3

The third sample profile is for a MAC algorithm that uses minimal power.

Profile Sample_3	
Primitive	MAC
Physical characteristics	Hardware implementation
Performance characteristics	Power ≤ 10 µW
Security characteristics	128-bit security, resistance against related key attacks, power analysis
Design goals	Resistance against tag forgeries

A sensor network node is an example of an application that may be compatible with profile Sample_3. Note that the same algorithm might be associated with both this profile and profile Sample_1.

3.3 Evaluation process

NIST will develop a submission and evaluation process for lightweight cryptographic algorithms that is similar to that of block cipher modes project [48]. There will be an open call for profiles and lightweight cryptographic algorithms. The submission requirements, guidelines, and sets of evaluation criteria will be made public on the Lightweight Cryptography project page (http://www.nist.gov/itl/csd/ct/lwc-project.cfm).

NIST will periodically hold workshops to discuss lightweight algorithms that are under consideration for the portfolio. These workshops will seek input from the community on cryptanalysis, implementations, and applications of the proposals.

The lwc-forum@nist.gov emailing list has been established for dialogue regarding NIST's Lightweight Cryptography project. To subscribe to the NIST lightweight cryptography mailing list, send an email message to lwc-forum-request@nist.gov, with a subject line "subscribe".

Tentative timeline:

- NIST solicits answers to the included list of questions about requirements from the community, based on current and upcoming application and device needs. Responses to the questions should be sent to lightweight-crypto@nist.gov with the subject line "Responses to questions on lightweight crypto requirements" before October 1, 2016. NIST will develop profiles based on the answers it receives, and these profiles will provide a starting point for discussion and call for primitives.
- NIST will hold the second Lightweight Cryptography Workshop on October 17-18, 2016. The purpose of this workshop will be to discuss this document, proposed profiles, comparison tools and methods, and recent work on cryptanalysis and implementations of lightweight cryptographic designs.
- NIST will publish a call for submissions of lightweight primitives in early 2017. The call will request submissions that are good solutions for the specified profiles.

578 - In late 2017, approximately six months after the call is published, NIST will begin
579 reviewing proposals.
580 - NIST will hold the third Lightweight Cryptography Workshop in early 2018 to discuss
581 proposals and plans for standardization.

582

References

[1] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T., *Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design andAnalysis*. Proc. 7th Annual International Workshop on Selected Areas in Cryptography (SAC 2000) Waterloo, Ontario, Canada, August 14–15, 2000, pp. 39-56, http://dx.doi.org/10.1007/3-540-44983-3_4

[2] Aumasson, J.-P., Henzen, L., Meier, W., and Naya-Plasencia, M., *Quark: A Lightweight Hash*, Journal of Cryptology, 2013, Vol. 26, (2), pp. 313-339, http://dx.doi.org/10.1007/s00145-012-9125-6

[3] Babbage, S., and Dodd, M., *The MICKEY Stream Ciphers*: 'New Stream Cipher Designs - The eSTREAM Finalists' (Springer, 2008), LNCS 4986, pp. 191-209, http://dx.doi.org/10.1007/978-3-540-68351-3_15

[4] Barker, E., and Roginsky, A., *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST Special Publication (SP) 800-131A Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland November 2015, http://dx.doi.org/10.6028/NIST.SP.800-131Ar1

[5] Barker, W.C., and Barker, E., *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication (SP) 800-67 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2012, http://dx.doi.org/10.6028/NIST.SP.800-67r1

[6] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L., *The SIMON and SPECK Families of Lightweight Block Ciphers*, IACR Cryptology ePrint Archive, 2013, http://eprint.iacr.org/2013/404

[7] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., and Verbauwhede, I., *SPONGENT: A Lightweight Hash Function*. Proc. 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), Nara, Japan, September 28 – October 1, 2011, LNCS 6917, pp. 312-325, http://dx.doi.org/10.1007/978-3-642-23951-9_21

[8] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., and Vikkelsoe, C., *PRESENT: An Ultra-Lightweight Block Cipher*. Proc. 9th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007), Vienna, Austria, September 10-13, 2007, LNCS 4727, pp. 450-466, http://dx.doi.org/10.1007/978-3-540-74735-2_31

[9] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., and Yalçın, T., *PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications*. Proc. 18th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012), Beijing, China, December 2-6, 2012, pp. 208-225, http://dx.doi.org/10.1007/978-3-642-34961-4_14

[10] Chen, L., *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, NIST Special Publication (SP) 800-108, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2009, http://dx.doi.org/10.6028/NIST.SP.800-108

[11] Chen, L., *Recommendation for Key Derivation through Extraction-then-Expansion*, NIST Special Publication (SP) 800-56C, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2011, http://dx.doi.org/10.6028/NIST.SP.800-56C

[12] Cryptographic Research and Evaluation Committees, http://www.cryptrec.go.jp/english/ [accessed August 11, 2016]

[13] Cryptographic Research and Evaluation Committees, *CRYPTREC Report 2014*, Report of the Cryptographic Technology Evaluation Committee, 296 pages, March 2015, http://www.cryptrec.go.jp/report/c14_eval_web.pdf

[14] Dang, Q., *Recommendation for Existing Application-Specific Key Derivation Functions*, NIST Special Publication (SP) 800-135 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2011, http://dx.doi.org/10.6028/NIST.SP.800-135r1

[15] De Cannière, C., and Preneel, B., *Trivium*: 'New Stream Cipher Designs - The eSTREAM Finalists' (Springer, 2008), LNCS 4986, pp. 244-266, http://dx.doi.org/10.1007/978-3-540-68351-3_18

[16] Dworkin, M., *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST Special Publication (SP) 800-38C, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2004, http://dx.doi.org/10.6028/NIST.SP.800-38C

[17] Dworkin, M., *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication* NIST Special Publication (SP) 800-38B, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2005, http://dx.doi.org/10.6028/NIST.SP.800-38B

[18] Dworkin, M., *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, NIST Special Publication (SP) 800-38D, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2007, http://dx.doi.org/10.6028/NIST.SP.800-38D

[19] ECRYPT, *eSTREAM: the ECRYPT Stream Cipher Project*, http://www.ecrypt.eu.org/stream/, [accessed August 10, 2016]

[20] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J., *Strong Authentication for RFID Systems Using the AES Algorithm*. Proc. 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Cambridge, MA, USA, August 11-13, 2004, pp. 357-370, http://dx.doi.org/10.1007/978-3-540-28632-5_26

[21] Gong, Z., Hartel, P., Nikova, S., Tang, S.-H., and Zhu, B., *TuLP: A Family of*

Lightweight Message Authentication Codes for Body Sensor Networks, Journal of Computer Science and Technology, 2014, Vol. 29, (1), pp. 53-68, http://dx.doi.org/10.1007/s11390-013-1411-8

[22] GS1 EPCglobal Inc., EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID, *Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHzVersion 2.0.1 Ratified*, 2015, http://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf

[23] Guo, J., Peyrin, T., and Poschmann, A., *The PHOTON Family of Lightweight Hash Functions*. Proc. 31st Annual International Cryptology Conference (CRYPTO 2011), Santa Barbara, CA, USA, August 14-18, 2011, pp. 222-239, http://dx.doi.org/10.1007/978-3-642-22792-9_13

[24] Guo, J., Peyrin, T., Poschmann, A., and Robshaw, M., *The LED Block Cipher*. Proc. 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), Nara, Japan, September 28 – October 1, 2011, pp. 326-341, http://dx.doi.org/10.1007/978-3-642-23951-9_22

[25] Hell, M., Johansson, T., and Meier, W., *Grain: A Stream Cipher for Constrained Environments*, International Journal of Wireless and Mobile Computing (IJWMC), 2007, Vol. 2, (1), pp. 86-93, http://dx.doi.org/10.1504/IJWMC.2007.013798

[26] Hirose, S., Ideguchi, K., Kuwakado, H., Owada, T., Preneel, B., and Yoshida, H., *A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW*. Proc. 13th International Conference on Information Security and Cryptology (ICISC 2010), Seoul, Korea, December 1-3, 2010, LNCS 6829, pp. 151-168, http://dx.doi.org/10.1007/978-3-642-24209-0_10

[27] Ideguchi, K., Owada, T., and Yoshida, H., *A Study on RAM Requirements of Various SHA-3 Candidates on Low-cost 8-bit CPUs*, IACR Cryptology ePrint Archive, 2009, http://eprint.iacr.org/2009/260

[28] ISO, ISO/IEC 29192-1:2012, *Information Technology – Security Techniques – Lightweight Cryptography – Part 1: General*, 2012, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56425

[29] ISO, ISO/IEC 29192-2:2012, *Information Technology – Security Techniques – Lightweight Cryptography – Part 2: Block Ciphers*, 2012, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56552

[30] ISO, ISO/IEC 29192-4:2013, *Information Technology – Security Techniques – Lightweight Cryptography – Part 4: Mechanisms Using Asymmetric Techniques*, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56427

[31] ISO, ISO/IEC 29167-1:2014, *Information Technology - Automated Identification and Data Capture Techniques – Part 1: Security Services for RFID Air Interfaces*, 2014,

693 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61128

694 [32] ISO, ISO/IEC 29167-11:2014, *Information Technology - Automated Identification and*
695 *Data Capture Techniques – Part 11: Crypto Suite PRESENT-80 Security Services for Air*
696 *Interface Communications*, 2014,
697 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60441

698 [33] ISO, ISO/IEC 29167-10:2015, *Information Technology - Automated Identification and*
699 *Data Capture Techniques – Part 10: Crypto Suite AES-128 Security Services for Air Interface*
700 *Communications*, 2015,
701 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60440

702 [34] ISO, ISO/IEC 29167-12:2015, *Information Technology - Automated Identification and*
703 *Data Capture Techniques – Part 12: Crypto Suite ECC-DH Security Services for Air Interface*
704 *Communications*, 2015,
705 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60442

706 [35] ISO, ISO/IEC 29167-13:2015, *Information Technology - Automated Identification and*
707 *Data Capture Techniques – Part 13: Crypto Suite Grain-128A Security Services for Air Interface*
708 *Communications*, 2015,
709 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60682

710 [36] ISO, ISO/IEC 29167-14:2015, *Information Technology - Automated Identification and*
711 *Data Capture Techniques – Part 14: Crypto Suite AES OFB Security Services for Air Interface*
712 *Communications*, 2015,
713 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61130

714 [37] ISO, ISO/IEC 29167-16:2015, *Information Technology - Automated Identification and*
715 *Data Capture Techniques – Part 16: Crypto Suite ECDSA-ECDH Security Services for Air*
716 *Interface Communications*, 2015,
717 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61321

718 [38] ISO, ISO/IEC 29167-17:2015, *Information Technology - Automated Identification and*
719 *Data Capture Techniques – Part 17: Crypto Suite CryptoGPS Security Services for Air Interface*
720 *Communications*, 2015,
721 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61942

722 [39] ISO, ISO/IEC 18000-63:2015, *Information technology - Radio frequency identification*
723 *for item management - Part 63: Parameters for air interface communications at 860 MHz to 960*
724 *MHz Type C*, 2015,
725 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63675

726 [40] ISO, ISO/IEC 29192-5:2016, *Information Technology – Security Techniques –*
727 *Lightweight Cryptography – Part 5: Hash-functions*, 2016,
728 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173

729 [41] Juels, A., and Weis, S.A., *Authenticating Pervasive Devices with Human Protocols*. Proc.

25th Annual International Cryptology Conference (CRYPTO 2005), Santa Barbara, California, USA, August 14-18, 2005, LNCS 3621, pp. 293-308, http://dx.doi.org/10.1007/11535218_18

[42] Leander, G., Paar, C., Poschmann, A., and Schramm, K., *New Lightweight DES Variants*. Proc. 14th International Workshop on Fast Software Encryption (FSE 2007), Luxembourg, Luxembourg, 2007, LNCS 4593, pp. 196-210, http://dx.doi.org/10.1007/978-3-540-74619-5_13

[43] Luykx, A., Preneel, B., Tischhauser, E., and Yasuda, K., *A MAC Mode for Lightweight Block Ciphers*. Proc. 23rd International Conference on Fast Software Encryption (FSE 2016), Bochum, Germany, March 20-23, 2016, LNCS 9783, pp. 43-59, http://dx.doi.org/10.1007/978-3-662-52993-5_3

[44] Mathew, S., Satpathy, S., Suresh, V., Anders, M., Kaul, H., Agarwal, A., Hsu, S., Chen, G., and Krishnamurthy, R., *340 mV-1.1 V, 289 Gbps/W, 2090-Gate NanoAES Hardware Accelerator With Area-Optimized Encrypt/Decrypt GF(2^4)^2 Polynomials in 22 nm Tri-Gate CMOS*, IEEE Journal of Solid-State Circuits, 2015, Vol. 50, (4), pp. 1048-1058, http://ieeexplore.ieee.org/ielx7/4/7066864/07019004.pdf?tp=&arnumber=7019004&isnumber=7066864

[45] Microchip Technology Inc., *New/Popular 8-bit Microcontrollers Products*, http://www.microchip.com/ParamChartSearch/chart.aspx?branchID=1012 [accessed August 9, 2016]

[46] Moradi, A., Poschmann, A., Ling, S., Paar, C., and Wang, H., *Pushing the Limits: A Very Compact and a Threshold Implementation of AES*. Proc. 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011), Tallinn, Estonia, May 15-19, 2011, LNCS 6632, pp. 69-88, http://dx.doi.org/10.1007/978-3-642-20465-4_6

[47] Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B., and Verbauwhede, I., *Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers*. Proc. 21st International Conference on Selected Areas in Cryptography (SAC 2014), Montreal, QC, Canada, August 14-15, 2014, pp. 306-323, http://dx.doi.org/10.1007/978-3-319-13051-4_19

[48] National Institute of Standards and Technology, *Block Cipher Modes*, http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html [accessed August 9, 2016]

[49] National Institute of Standards and Technology, *Post-Quantum Crypto Project*, http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html, [accessed 2016, August 11]

[50] National Institute of Standards and Technology, *NIST Cryptographic Standards and Guidelines Development Process*, NISTIR 7977, March 2016, http://dx.doi.org/10.6028/NIST.IR.7977

[51] Needham, R.M., and Wheeler, D.J., *Tea extensions*, Technical Report, Computer Laboratory, University of Cambridge, October 1997, http://www.cix.co.uk/~klockstone/xtea.pdf

766 [52] NXP, *8-bit RS08*, http://www.nxp.com/products/microcontrollers-and-processors/more-
767 processors/8-16-bit-mcus/8-bit-rs08:RS08FAMILY [accessed August 9, 2016]

768 [53] Osvik, D.A., Bos, J.W., Stefan, D., and Canright, D., *Fast Software AES Encryption*.
769 Proc. 17th International Workshop on Fast Software Encryption (FSE 2010), Seoul, Korea,
770 February 7-10, 2010, LNCS 6147, pp. 75-93, http://dx.doi.org/10.1007/978-3-642-13858-4_5

771 [54] Poschmann, A.Y.: *Lightweight Cryptography: Cryptographic Engineering for a*
772 *Pervasive World*. Ph.D. Thesis, Ruhr University Bochum, 2009, http://d-nb.info/996578153

773 [55] Renesas Electronics Corporation, *RL78 Family*, https://www.renesas.com/en-
774 us/products/microcontrollers-microprocessors/rl78.html, [accessed August 11, 2016]

775 [56] Rivest, R.L., *The RC5 Encryption Algorithm*. Proc. Second International Workshop on
776 Fast Software Encryption (FSE 1994), Leuven, Belgium, December 14–16, 1994, LNCS 1008,
777 pp. 86-96, http://dx.doi.org/10.1007/3-540-60590-8_7

778 [57] Saarinen, M.-J.O., and Engels, D.W., *A Do-It-All-Cipher for RFID: Design Requirements*
779 *(Extended Abstract)*, IACR Cryptology ePrint Archive, 2012, http://eprint.iacr.org/2012/317

780 [58] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., and Shirai, T., *Piccolo:*
781 *An Ultra-Lightweight Blockcipher*. Proc. 13th International Workshop on Cryptographic
782 Hardware and Embedded Systems (CHES 2011), Nara, Japan, September 28 – October 1, 2011,
783 pp. 342-357, http://dx.doi.org/10.1007/978-3-642-23951-9_23

784 [59] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T., *The 128-Bit Blockcipher*
785 *CLEFIA (Extended Abstract)*. Proc. 14th International Workshop on Fast Software Encryption
786 (FSE 2007), Luxembourg, Luxembourg, March 26-28, 2007, pp. 181-195,
787 http://dx.doi.org/10.1007/978-3-540-74619-5_12

788 [60] Sönmez Turan, M., Barker, E., Burr, W., and Chen, L., *Recommendation for Password-*
789 *Based Key Derivation: Part 1: Storage Applications*, NIST Special Publication (SP) 800-132,
790 National Institute of Standards and Technology, Gaithersburg, Maryland, December 2010,
791 http://dx.doi.org/10.6028/NIST.SP.800-132

792 [61] Suzaki, T., Minematsu, K., Morioka, S., and Kobayashi, E., *TWINE: A Lightweight Block*
793 *Cipher for Multiple Platforms*. Proc. 19th International Conference on Selected Areas in
794 Cryptography (SAC 2012), Windsor, ON, Canada, August 15-16 2012, pp. 339-354,
795 http://dx.doi.org/10.1007/978-3-642-35999-6_22

796 [62] Texas Instruments, *COP912C 8-Bit Microcontroller*,
797 http://www.ti.com/product/COP912C [accessed August 9, 2016]

798 [63] U.S. Department of Commerce, *Advanced Encryption Standard (AES)*, Federal
799 Information Processing Standards (FIPS) Publication 197, November 2001,
800 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[64] U.S. Department of Commerce, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards (FIPS) Publication 198-1, July 2008, http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[65] U.S. Department of Commerce, *Secure Hash Standard (SHS)* Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, http://dx.doi.org/10.6028/NIST.FIPS.180-4

[66] U.S. Department of Commerce, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, Federal Information Processing Standards (FIPS) Publication 202, August 2015, http://dx.doi.org/10.6028/NIST.FIPS.202

[67] Université du Luxembourg, *Lightweight Block Ciphers*, https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers, [accessed May 10, 2016]

[68] Wheeler, D.J., and Needham, R.M., *TEA, A Tiny Encryption Algorithm*. Proc. Second International Workshop on Fast Software Encryption (FSE 1994), Leuven, Belgium, December 14–16, 1994, LNCS 1008, pp. 363-366, http://dx.doi.org/10.1007/3-540-60590-8_29